

CLAIMS

What is claimed is:

1. A method of authenticating a wireless device for accessing a first wireless network challenging said device, comprising:

5 receiving an authentication challenge from said first wireless network at a first wireless device;

forwarding said authentication challenge from said first wireless device to a second wireless device storing an authentication key;

10 calculating an authentication response based on said authentication key at said second wireless device;

forwarding said authentication response from said second wireless device to said first wireless device; and

transmitting said authentication response from said first wireless device to said first wireless network.

2. The method of claim 1 wherein said second wireless device is a wireless communication mobile terminal.

3. The method of claim 1 wherein receiving said authentication challenge and
20 transmitting said authentication response occur across a wireless communication interface.

4. The method of claim 3 wherein said wireless communication interface is a wireless local area network interface.

25

5. The method of claim 1 wherein forwarding said authentication challenge and forwarding said authentication response occur across a communication interface connecting said first and second wireless devices.

6. The method of claim 5 wherein said communication interface is a wire or optical cable interface.

7. The method of claim 5 wherein said communication interface is a wireless communication interface.

8. The method of claim 7 wherein said wireless communication interface is an optical interface.

9. The method of claim 7 wherein said wireless communication interface is a radio frequency interface.

10. The method of claim 9 wherein said radio frequency interface is a BLUETOOTH interface.

11. The method of claim 1 wherein said authentication key is a private key, and wherein said authentication challenge is generated based on a public key associated with said private key.

12. The method of claim 1 wherein calculating an authentication response based on said authentication key comprises performing a mathematical operation on said

authentication challenge using said authentication key to obtain said authentication response.

13. The method of claim 1 further comprising authenticating said first wireless device
5 by said first wireless network based on said authentication response.

14. The method of claim 13 wherein said authentication key comprises a shared key known to said first wireless network.

10 15. The method of claim 14 wherein authenticating said first wireless device by said first wireless network comprises:

using said authentication challenge and said shared key to compute an expected authentication response at said first wireless network; and

15 comparing said expected authentication response with the actual authentication response received from said first wireless device.

16. The method of claim 13 wherein said authentication key is a private key known only to the second wireless device, and wherein said private key has a corresponding public key that is known to the first wireless network.

20 17. The method of claim 16 wherein said first wireless network encrypts a data pattern using said public key to generate the authentication challenge, and wherein authenticating said first wireless device by said first wireless network further comprises comparing the authentication response to the original data pattern used to generate the
25 authentication challenge.

18. The method of claim 17 wherein calculating an authentication response based on said authentication key comprises decrypting said authentication challenge to obtain the data pattern.

19. The method of claim 14 further comprising:
generating said authentication challenge at a second wireless network ;
forwarding said authentication response from said first wireless network to said
second wireless network; and
5 authenticating said first wireless device by said second wireless network based
on said authentication response.

20 The method of claim 19 further comprising:
sending an authentication result from the second wireless network to the first
10 wireless network; and
providing or denying access for the first wireless device to the first wireless
network based on said authentication result.

21. The method of claim 19 wherein said authentication key comprises a shared key
15 known to said second wireless network.

22. The method of claim 21 wherein authenticating said first wireless device by said
second wireless network comprises:
using said authentication challenge and said shared key to compute an expected
20 authentication response at said second wireless network; and
comparing said expected authentication response with the actual authentication
response received from said first wireless network.

23. The method of claim 19 wherein said authentication key is a private key known
25 only to the second wireless device, and wherein said private key has a corresponding
public key that is known to the second wireless network.

24. The method of claim 23 wherein said second wireless network encrypts a data pattern using said public key to generate the authentication challenge, and wherein authenticating said first wireless device by said second wireless network further
5 comprises comparing the authentication response to the original data pattern used to generate the authentication challenge.

25. The method of claim 19 wherein said second wireless network is a wireless communication network.

10 26. A wireless device comprising:
a first interface to communicate with a wireless network;
a second interface to communicate with a provisioned wireless device having an authentication key used to access the wireless network;
15 a microprocessor connected to said first and second interfaces and programmed to:
forward an authentication challenge received from the wireless network via said first interface to the provisioned wireless device via said second interface;
20 receive an authentication response from the provisioned wireless device via said second interface; and
forward the authentication response via said first interface to the wireless network.

25 27. The wireless device of claim 26 wherein the first interface is a WLAN interface.

28. The wireless device of claim 26 wherein the second interface is wireless interface.

29. The wireless device of claim 28 wherein the second interface a radio frequency
5 interface.

30. The wireless device of claim 29 wherein the second interface is a BLUETOOTH interface.

Coats & Bennett

31. A wireless device having an authentication key used to access a wireless network comprising:

an interface to communicate with a non-provisioned wireless device;

an authentication unit connected to said interface and having a memory for

storing the authentication key and a processor for performing calculations

using said authentication key, said authentication unit being operative to:

receive an authentication challenge via said interface from the non-

provisioned wireless device attempting to access the wireless

network,

compute an authentication response using the authentication challenge

and the authentication key; and

forward the authentication response via the interface to the non-

provisioned wireless device to be used by the non-provisioned

wireless device to access the wireless network.

32. The wireless device of claim 31 wherein the interface is a wireless interface.

33. The wireless device of claim 32 wherein the interface a radio frequency interface.

34. The wireless device of claim 33 wherein the interface is a BLUETOOTH interface.